

# **Principper for privacy**

Udgivet af: ITEK og Dansk Industri  
Redaktion: Henning Mortensen  
ISBN: 87-7353-602-4  
0.07.06

## **Summary**

Privacy har været genstand for opmærksom blandt mange parter – i særdeleshed for OECD, Europarådet, EU og nationale lovgivere. Dette arbejde har dels ført til overvejelser om, hvad privacy er og dels ført til en konkret implementering af de bestemmelser, der vedrører data og kommunikation i persondataloven, som administreres af Datatilsynet.

I dette notat identificeres de konkrete principper, det undersøges, hvordan disse er implementeret i Persondataloven og endelig sammenfattes principperne i notatets sammenfatning. På denne baggrund bør det være muligt at vurdere, hvilke principper der skal fokuseres på ved en eventuel udarbejdelse af en privacykodeks for it-leverandører.

## **Baggrund**

ITEK og Dansk Industri har fundet det interessant at beskæftige sig med privacy, fordi det er afgørende for samfundets effektivisering og teknologiens anvendelighed, at vi skaber sikkerhed og tryghed for borgere og virksomheder, når de anvender moderne elektronisk kommunikationsteknologi. Dette er specielt relevant netop nu, fordi vi i disse år oplever en eksplosion i mængden af elektronisk registreret information. ITEK og Dansk Industri har derfor i samarbejde med en lang række interessenter taget initiativ til at formulere dette og flere andre notater på privacy området. De involverede parter har været: Forbrugerrådet, Finansrådet, Institut for Menneskerettigheder, Digital Rights, AIM Danmark, TDC A/S, Siemens A/S, Microsoft Danmark A/S, Nensome ApS, Zebranet ApS, LOGISYS A/S, Parkegaard og Kristensen Sikkerhed ApS, RFIDsec ApS og CSIS ApS.

I mange år har ikt-erhvervet talt om de muligheder private forbrugere en gang i fremtiden ville få med anvendelse af trådløse teknologier. I dag er mange af disse teknologier en realitet og velkendte blandt forbrugerne - f.eks. mobiltelefoner, trådløse computernetværk i hjemmet og infrarøde porte på computere. Disse velkendte eksisterende teknologier vil få mange flere anvendelsesområder i den nære fremtid.

Fremtiden vil give mulighed for, at man kan få personligt tilrettet information overalt, hvor man befinder sig. Vi vil komme til at opleve intelligente netværkszoner, som vil kunne opsamle og registrere vores tilstedeværelse, registrere vores adfærd og behov og på denne baggrund give os forskellige relevante valg eller give os hjælp til at indfri forskellige behov. Dette tilvejebringes af de trådløse teknologier og en række nye sensorer.

Andre teknologier betyder, at man i dag kan lagre og behandle enorme mængder af data til relativt lave omkostninger. Det betyder, at kapacitet ikke længere er en knap ressource - i hvert fald ikke i den vestlige verden. Teknologierne hertil er de velkendte harddisk- og processorteknologier – som enkeltsystemer eller i form af grid computing.

På softwaresiden er computere med årene blevet stadig bedre til at genkende mønstre og på baggrund af disse vide, hvad der er mest hensigtsmæssigt at foretage sig. Sådanne selv-lærende systemer eller direkte kunstig intelligens vil blive anvendt i flere og flere sammenhænge.

De teknologier, som kan bruges til at genkende mennesker, er også gennem de senere år blevet meget udviklet og har i dag nået et modenhedsniveau, hvor de reelt er klar til at slå igennem på markedet. De biometriske teknologier kan genkende på baggrund af iris, hånd- eller fingeraftryk, venemønster, hovedform, gangart, vægt, temperatur, DNA, stemme og flere andre ting. Det betyder, at en person under bestemte omstændigheder kan identificeres eller at personens påståede eller antagne identitet kan genkendes/verificeres.

Endelig er det en vigtig udvikling at alle de nævnte teknologier til stadighed kræver fysisk mindre komponenter, som kan produceres til stadigt lavere priser. Det gør at sensorer og transmittorer kan placeres i en lang række bærbare apparater med forskellig funktionalitet. Vi kan med en fælles betegnelse kalde det for mikro- og nanoteknologierne.

Intelligente netværk, sensorer, forbedret lagring og behandling, selvlærende systemer, biometri og miniaturisering er alle teknologiske innovationer, som er i gang med at gøre vores tilværelse lettere og vil kunne give os oplevelser, som ikke før var muligt.

Den skitserede teknologiske udvikling kan imidlertid ikke stå alene. Den bør følges af en udvikling i, hvordan mennesker har kendskab til, opfatter og forstår den nye teknologi. Hvordan mennesker accepterer og ønsker at anvende teknologien. Hvordan mennesker forstår teknologiens risici og konsekvenser og i praksis håndterer disse.

Det bør også følges af spørgsmålet om, hvilke reelle muligheder mennesker har for at sikre deres privacy med de løsninger, der produceres med funktionalitet for øje, og som ikke i alle tilfælde tager hensyn til privacy. I stedet for at udbyde en løsning, der faktisk kan privacyenables, stilles mennesket ofte overfor et valg mellem at anvende en teknologi, der opfylder hans formål, men som er uden privacy, eller slet ikke at anvende teknologien og dermed ikke få opfyldt sit formål.

Hertil kommer at teknologier typisk udvikles og udbredes med en global markedsplads for øje, og i sagens natur ikke tager højde for de forskellige værdier og normer, der hersker forskellige steder i den globale landsby. Dermed vil der mange steder ikke automatisk være forståelse og accept af samt tillid til, den måde teknologierne er indrettet på.

## **Formål**

Dette papir har til formål at stimulere en offentlig dansk debat om menneskers privacy behov og rettigheder i relation til teknologianvendelse. Privacy kan påvirkes af en række faktorer, som overordnet er lovning, selvregulering i form af f.eks. et Code of Conduct og endelige teknologiuudvikling, -implementering og -anvendelse<sup>1</sup>.

Samtidig er papiret også en opfordring til teknologileverandørerne om at efterleve de skitserede principper. Man kan sige, at hensigten er, at dette skal være grundlaget for eventuelt at udarbejde en

---

<sup>1</sup> På en workshop i Dansk Industri i foråret 2006 identificeredes en række forhold, som værende af betydning for privacy. Disse forhold kan groft set rubriceres under nedenstående hovedoverskrifter:

- Awareness (gør det muligt for individet at træffe rationelle valg om egen privacy)
- Selvregulering i branchen (Code of Conduct)
- Lovgivning (traktater, grundlov, persondatalov og særlige tilfælde af samtykke)
- Globalisering (f.eks. forskellige krav i EU/USA og forskellige lande)
- Teknik (især privacyenabling af eksisterende teknologier og privacyudviklingsmodel for nye teknologier, designe risici væk, channel management svarende til vurdering af, hvornår vil man give hvilke data væk)
- Offentlige investeringer (krav til privacy i leverancer)
- Individets ansvar (Beskyttelse af grundlæggende værdier)
- Standarder
- Individets ejendomsret til data (empowerment: 1. individuelle kompetencer i form af viden og værktøjer, 2. dataadgang i form af muligheden for at åbne op for adgang til offentligt lagrede data, 3. kontrol med individuelle data)
- Etik (andre værdier)
- Markedskræfter versus makroøkonomiske hensyn

”Code of Conduct” eller ”Best Practise” for, hvordan teknologileverandørerne bør privacyenable deres eksisterende produkter og services, og hvordan systemejere og designere bør tænke privacy ind i udviklingen og anvendelsen af fremtidige produkter.

Punkterne i dette notat er foranderlige med den meget hastige teknologiske udvikling og de deraf affødte nye teknologier, nye services, nye processer og nye kombinationer heraf, som kommer på markedet i de kommende år.

Notatet har ikke til formål at gennemgå og opsummere de forskellige former for teknologier som findes rundt omkring. I brede termer kan vi dog fremhæve, at der er tænkt på teknologiske begreber som f.eks. "pervasive computing", "location based services", "intelligente trådløse netværkszoner", "mobile services", "RFID", "biometri" og "Bluetooth".

Notatet har heller ikke til formål at beskrive cases for de forskellige teknologiers implementering. Dette findes der allerede glimrende eksempler på andre steder.

### **Privacydefinition**

Teknologierne er enablere for muligheder. Hvilke muligheder vi har, er det kun fantasien og fysikken, der sætter grænser for. Den måde, som mulighederne tilvejebringes på, er imidlertid af stor betydning for, om menneskene ønsker at benytte dem. De teknologiske muligheder skal sammenholdes med processer, som tager hensyn til de grundlæggende rettigheder, som menneskene har.

I hvilke sammenhænge kan menneskene have fordel af, at deres tilstedeværelse registreres, hvordan og af hvem? Hvilken adfærd er det rimeligt at registrere hvornår, med hvilken henførbarehed til det enkelte menneske og til hvilket formål? Hvordan beskytter man mod risici for afsløring af oplysninger uden at etablere nye risici? Hvilke muligheder er det rimeligt, at teknologien foreslår, hvornår og til hvilke grupper af mennesker? Hvilke behov er det rimeligt at indfri i en given situation og med hvilke midler?

Svarene på disse spørgsmål er helt grundlæggende relateret til retten til privatlivets fred - herunder også vedrørende persondata. Man kan sige, at det vedrører hvor langt samfundet kan gå i forhold til indblanding i en persons private forhold. På den måde vedrører privacy alle menneskerettighederne. Der findes ikke en entydig definition af privacy. Men man kan udlede, hvad det drejer sig om ved at se på, hvordan andre tidligere har forsøgt at indkredse emnet<sup>2</sup>.

Den ældste henvisning til privacy findes hos den senere amerikanske højesteretsdommer, Louis Brandeis, som i slutningen af 1800-tallet beskrev det som retten til at være alene<sup>3</sup>. Denne definition er senere blevet anvendt i rapporter fra Metagroup og Deloitte til henholdsvis Ministeriet for Videnskab, Teknologi og Udvikling og Nordisk Råd. Robert Ellis Smith, som er redaktør for Privacy Journal, har defineret privacy som det individuelle behov for et fysisk frirum, hvor vi kan vide os sikre for ikke at blive udsat for forstyrrelser, indtrængning, blive sat i forlegenhed eller blive holdt ansvarlig for vores

---

<sup>2</sup> Et af de mest sprogligt svulstige eksempler findes hos det engelske parlamentsmedlem William Pitt som i sin tale ved Excise Bill I 1763 skrev: "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement", Privacy & Human Rights, udgivet af EPIC, 2003, p. 5.

<sup>3</sup> Samuel Warren and Louis Bradeis, The Right to privacy, 4 Harvard Law review, 193-220 (1890), citeret fra Privacy & Human Rights, udgivet af EPIC, 2003, p. 2 og 6. Originalteksten kan findes her: <http://www.louisville.edu/library/law/brandeis/privacy.html>

handlinger, og hvor vi gerne vil kunne kontrollere og vide tidspunktet for og måden hvorpå, personlig information om os selv kommer til andres kendskab<sup>4</sup>.

EPIC<sup>5</sup> skitserer den del af privacy, der vedrører personlige data som værende den internationale konsensus, der vedrører retten til at indsamle, vedligeholde, anvende, videregive/transmittere og behandle personlig information<sup>6</sup>.

Den engelske tænketank, DEMOS, som forsker i demokrati og demokratiske principper, har denne interessante definition, som inkluderer psykologiske aspekter, af privacy: "Privacy can best be understood as a protection against certain kinds of risks - risks of injustice through such things as unfair inference, risks of loss of control over personal information, and risks of indignity through exposure and embarrassment"<sup>7</sup>.

Også forskellige standarder beskæftiger sig med privacy. I Common Criteria standarden<sup>8</sup>, som er en model til at vurdere om et stykke software er tilstrækkeligt sikkert, hedder det: Privacy "requirements provide a user protection against discovery and misuse of identity by other users"<sup>9</sup>. Privacy dekomponeres så til fire elementer: anonymitet (brugerens fysiske identitet må ikke kunne etableres), pseudonymitet (brugerens identitet kan ikke afsløres, men brugeren kan stadig gøres ansvarlig for sine handlinger), unlinkability (det skal være muligt at afgøre, om den samme bruger lavede forskellige handlinger på et givent system) og unobservability (det skal være umuligt at afgøre, om en bruger har foretaget en bestemt handling). I standarderne for informationssikkerhed<sup>10</sup> er der ligeledes formuleret krav til beskyttelse af personoplysninger. I DS484 hedder det: "Personoplysninger, dvs. enhver form for information om en identificeret eller identificerbar fysisk person, skal beskyttes i overensstemmelse med gældende lovgivning og eventuelle kontraktlige forpligtelser"<sup>11</sup>. I denne sammenhæng tænkes der især på "Lov om behandling af personoplysninger", som implementerer EU's persondatadirektiv.

Endelig er beskyttelsen af privacy fastlagt i international regulering<sup>12</sup>. Først og fremmest i FN's Verdenserklæring om Menneskerettigheder fra 1948, hvor det i artikel 12 hedder: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"<sup>13</sup>. Desuden er privacy fastlagt i Den Europæiske Menneskerettighedskonvention<sup>14</sup> fra 1950,

---

<sup>4</sup> Robert Ellis Smith, Ben Franklin's Web Site 6 (Sheridan Books 2000), citeret fra Privacy & Human Rights, udgivet af EPIC, 2003, p. 2.

<sup>5</sup> EPIC står for Electronic Privacy Information Center, og er formodentlig USA's mest indflydelsesrige privacyorganisation.

<sup>6</sup> <http://www.epic.org/reports/dmfprivacy.html>

<sup>7</sup> <http://www.demos.co.uk/catalogue/thefutureofprivacyvolume1>

<sup>8</sup> Common Criteria er en ISO-standard ved navn: ISO/IEC 15408:2005, og den kan i sin fulde længde findes på <http://www.commoncriteriaportal.org>. Privacy-kravene fremføres i standardens 2. del: "Security functional requirements", <http://www.commoncriteriaportal.org/public/files/ccpart2v2.3.pdf>. De krav der omtales, kan definatorisk sammenlignes med andre anvendelser af ordene i denne artikel fra Technische Universität Dresden, [http://dud.inf.tu-dresden.de/literatur/Anon\\_Terminology\\_v0.28.pdf](http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf).

<sup>9</sup> <http://www.commoncriteriaportal.org/public/files/ccpart2v2.3.pdf>, p. 116 - 124.

<sup>10</sup> Der eksisterer en lang række forskellige standarder for informationssikkerhed, der adresserer privacy. I de konkrete tilfælde tænkes der på formuleringerne i ISO/IEC17799:2005 og DS484:2005.

<sup>11</sup> DS484, kontrolpunkt 15.1.4.

<sup>12</sup> Bemærk at nogle af disse dokumenter er juridisk bindende, mens andre er politiske hensigtserklæringer. Typisk er konventionerne juridisk bindende.

<sup>13</sup> <http://www.un.org/Overview/rights.html>

<sup>14</sup> Originaltitlen er i oversættelse: "Konvention til beskyttelse af Menneskerettigheder og grundlæggende Frihedsrettigheder" og kan findes på <http://www.menneskeret.dk/menneskeretieuropa/konventionen/selveemrk/>. Den engelske originaltekst kan findes her: <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>. Kilden til denne er

hvor det i artikel 8, stk. 1, som omhandler "Ret til respekt for privatliv og familieliv", hedder: "Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.". Disse to formuleringer er rimeligt overensstemmende. Imidlertid har Den Europæiske menneskerettighedskonvention en undtagelsesbestemmelse fra artiklens stk. 1 i artiklens stk. 2, hvor det hedder: "Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder".

Både Verdenserklæringen og den Europæiske Menneskerettighedskonvention indeholder også retningslinier for beskyttelse af ytringsfriheden. Hos FN er formuleringen placeret i artikel 19, hvor det hedder: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". Den tilsvarende formulering i Den Europæiske menneskerettighedskonvention findes i artikel 10, stk. 1, hvori det hedder: " Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til landegrænser". Senere i stk. 1 og i stk. 2, kommer der så en række undtagelser<sup>15</sup>.

På baggrund af disse politiske dokumenter har en række nationalstater eller grupper af lande vedtaget forskellige erklæringer, som er baseret på disse principper. En stor del af disse er dog udformet i den vestlige verden og tager derfor ikke hensyn til lokale kulturelle eller etiske forskelligheder i verdenssamfundet.

I den danske Grundlov reflekteres principperne også<sup>16</sup>. Retten til at kommunikere fastslås i § 72: " Boligen er ukrænkelig. Husundersøgelser, beslaglæggelse og undersøgelse af breve og andre papirer samt brud på post-, telegraf- og telefonhemmeligheden må, hvor ingen lov hjemler en særegen undtagelse, alene ske efter en retskendelse." og ytringsfriheden fastslås i § 77: "Enhver er berettiget til på tryk, i skrift og tale at offentliggøre sine tanker, dog under ansvar for domstolene. Censur og andre forebyggende forholdsregler kan ingensinde på ny indføres".

Som supplement til de egentlige definitioner kan det fremhæves, at der traditionelt sondres mellem fire typer privacy<sup>17</sup>:

- Informations privacy, som vedrører indsamlingen og behandlingen af personlig information - også kaldet databeskyttelse

---

Europarådet, <http://www.coe.int>, hvis formål er: "Europarådets overordnede mål er at opnå større enhed mellem de 46 medlemsstater med henblik på at sikre den personlige og politiske frihed samt retsstatsprincippet, der er grundlaget for et ægte demokrati, og som berører alle europæeres liv på mange forskellige måder. Alle medlemsstater er forpligtet til at gøre frihed, menneskelig værdighed og den enkeltes velfærd til faste principper for regeringens politik.", <http://www.coe.int/dk/portal/?L=DK>.

<sup>15</sup> Den samlede artikel 10 lyder: "Stk. 1. Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker, uden indblanding fra offentlig myndighed og uden hensyn til landegrænser. Denne artikel forhindrer ikke stater i at kræve, at radio-, fjernsyns- eller filmforetagender kun må drives i henhold til bevilling.

Stk. 2. Da udøvelsen af disse frihedsrettigheder medfører pligter og ansvar, kan den underkastes sådanne formaliteter, betingelser, restriktioner eller straffebestemmelser, som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed, territorial integritet eller offentlig tryghed, for at forebygge uorden eller forbrydelse, for at beskytte sundheden eller sædeligheden, for at beskytte andres gode navn og rygte eller rettigheder, for at forhindre udsprede af fortrolige oplysninger, eller for at sikre domsmagtens autoritet og upartiskhed."

<sup>16</sup> <http://www.grundloven.dk/>.

<sup>17</sup> Privacy & Human Rights, udgivet af EPIC, 2003, p. 3.

- Kropslig privacy, som vedrører retten til at beskytte sin fysiske krop mod f.eks. genetiske tests
- Kommunikationsprivacy, som vedrører sikkerhed og privacy i forhold til breve, mail, telefonopkald, internetanvendelse og lignende
- Territorial privacy, som vedrører grænsedragningen mellem det private miljø og andre miljøer f.eks. på arbejdspladsen og i det offentlige rum - herunder f.eks. videoovervågning og ID tjek.

Vi oplever dog en udvikling, hvor de forskellige typer privacy smelter sammen fordi teknologierne bygger bro mellem tid og sted. Dette aktualiserer betydningen af at beskæftige sig med privacy.

### **Kilder**

Privacy er noget som rigtig mange interessenter har beskæftiget sig med. På den danske scene har vi primært set Institut for Menneskerettigheder, virksomheden Priway og Datatilsynet, som fører tilsyn med persondataloven.

Internationalt har arbejdet med privacy været i gang længe. I de engelsktalende lande har man fortrinsvis talt om ”privacy”, mens man på det europæiske fastland har talt om persondatabeskyttelse. Privacy har et bredere indhold end persondatabeskyttelse, idet også beskyttelse af privatsfæren og kroppen synes at høre herunder. I dette arbejde vil vi fastholde ordet privacy for at tydeliggøre at de moderne teknologier handler om andet og mere end beskyttelser af databaser eller kartoteker med personhenførbare oplysninger.

Da udvekslingen af data i stigende grad foregår på tværs af grænser, da mange virksomheder arbejder internationalt og da det internationale arbejde i høj grad har inspireret det danske, har vi valgt fortrinsvis at basere dette notat på den internationale indsats. Vi har valgt at fokusere på resultaterne fra de internationale organisationer: OECD, Europarådet og EU, på de to største privacy-organisationer: EPIC (som er amerikansk) og Privacy International (som er engelsk baseret) og endelig på en række forskningsresultater fortrinsvis fra Simson Garfinkel, der har en PhD i privacy fra MIT.

Det skal bemærkes, at også FN har været aktive på privacyområdet idet privacy var tema på FNs Verdenstopmøde om Informationsamfundet (WSIS), der blev afholdt i 2003 i Geneve og 2005 i Tunis. Geneve topmødet resulterede i en politisk deklaration og handlingsplan, hvor privacy indgår som tema i aktionslinien C5: ”Building confidence and security in the use of ICTs”, med ITU som international koordinator<sup>18</sup>. Formuleringerne er dog ret brede, så vi vil ikke her forfølge FN’s bidrag yderligere.

Baggrunden for alle de nævnte initiativer er, at man ønsker at regulere den situation, hvor individerne ikke længere er anonyme. Når individerne ikke er anonyme, kan man henhøre oplysninger om dem til deres person, og det er netop dette, der anses for at være ubehageligt og resulterer i risiko og i manglende sikkerhed for individerne, fordi man kan danne sig et samlet indtryk af en person, misbruge oplysningerne til kriminalitet eller få adgang til oplysninger, som personen betragter som fortrolige. Man kan sige, at initiativerne specificerer den maksimale henførbarehed, der må være af oplysninger om personer tillige med, hvordan denne skal implementeres. Dermed er det overordnede princip, at borgerne skal have kontrol med egne data gennem så lidt identifikation og linkbarhed som muligt.

### *OECD*

OECD har beskæftiget sig med emnet i mange år. Årsagen er, at man allerede i 70’erne forudså, at der for at udnytte fremtiden teknologiske muligheder effektivt var et stigende behov for udveksling af personlige data på tværs af nationale grænser. Hertil kom, at de nationale myndigheder begyndte at indrette forskellige typer lovgivning ud fra nationale hensyn. Da de nationale hensyn var forskellige fra

<sup>18</sup> <http://www.itu.int/wsis/docs/geneva/official/poa.html>.

land til land begyndte lovgivningerne i stigende grad at være forskellige. For at opnå effektivitet og convenience gevinst tillige med en harmonisering af national lovgivning på den ene side, men samtidig lade dette ske under hensyn til menneskerettighederne på den anden side, producerede OECD et sæt guidelines, som nationalstaterne kunne anvende ved udformning af deres lovgivning. Desuden har OECD senere genereret en såkaldt privacy policy generator, som kan bruges af myndigheder, organisationer og virksomheder til på baggrund af en række spørgsmål at generere en privacy politik for anvendelse af deres online elektroniske tjenester.

Kilderne fra OECD er:

1. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)<sup>19</sup>
2. Declaration on Transborder Data Flows (1985)<sup>20</sup>
3. Ministerial Declaration on the Protection of Privacy on Global Networks (1998)<sup>21</sup>
4. OECDs privacy policy generator<sup>22</sup> og OECDs egen privacy politik<sup>23</sup>.

Blandt disse kilder er det især den første, som er relevant, idet den definerer de grundlæggende retningslinier, som det øvrige arbejde er baseret på. I denne guideline opstilles otte principper, som privacy skal opfylde. Principperne uddybes i de detaljerede bemærkninger til guidelinen.

### 1. **Princippet om begrænset indsamling**

Der skal være begrænsninger på indsamlingen af personlige data. Data skal indsamles på en fair måde og i overensstemmelse med lovgivningen. Hvor det anses for passende, skal det ske med viden og accept fra den, som data vedrører.

*Begrænsningerne er ikke universelle, men beror bl.a. på det formål, hvortil data indsamles, kvaliteten af data, klassificering af data, adgangen til data og almindelige menneskerettighedshensyn.*

*At indsamlingen skal ske på en fair måde betyder, at det som hovedregel ikke må holdes skjult for den data vedrører, at data indsamles.*

*De steder, hvor der kan indhentes accept, bør det også ske, men f.eks. i forbindelse med kriminel efterforskning kan det være en fordel for samfundet at hemmeligholde indsamlingen. I forbindelse med umyndige personer kan accept gives af formynder.*

### 2. **Princippet om datakvalitet**

Personlige data skal være relevante for det formål, hvortil de anvendes. I den grad det er nødvendigt for formålet, skal data være præcise, komplette og være opdateret.

*Relevansen vedrører sikkerheden for, at data, som er indsamlet til et formål, ikke misbruges til andre formål og dermed kan være med til at give et forkert billede af virkeligheden - f.eks. i forbindelse med opinionsundersøgelser.*

*Præcision, kompletthed og det at data stadig er opdateret betyder, at data skal give et retvisende billede af den, som data vedrører, og at dette retvisende billede kun kan anses for retvisende på det tidspunkt, data blev indsamlet.*

### 3. **Princippet om formålsspecificering**

Formålet, for hvilket data indsamles, skal være præciseret senest på det tidspunkt, hvor indsamlingen foregår. Senere anvendelse af data skal være i overensstemmelse med det oprindelige formål eller andre formål, der er komplementære til det oprindelige formål. Hver gang formålet ændres, skal det nye formål specificeres.

*Formålet med indsamling af data må ikke være vilkårligt og skal være kendt af dem, der afgiver*

<sup>19</sup> [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).

<sup>20</sup> [http://www.oecd.org/document/25/0,2340,en\\_2649\\_34255\\_1888153\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/25/0,2340,en_2649_34255_1888153_1_1_1_1,00.html).

<sup>21</sup> <http://www.oecd.org/dataoecd/39/13/1840065.pdf>.

<sup>22</sup> <http://www.oecd.org/sti/privacygenerator>.

<sup>23</sup> [http://www.oecd.org/document/40/0,2340,en\\_2649\\_201185\\_1899048\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/40/0,2340,en_2649_201185_1899048_1_1_1_1,00.html).

*data. Annonceringen af dette kan ske på mange måder, men det er vigtigt, at man ved, at dem, der afgiver data, var informeret.*

*Når data ikke længere anvendes, bør de, hvis det er muligt, destrueres eller anonymiseres således, at de som følge af manglende interesse ikke udsættes for reduceret beskyttelse og kan falde i uvedkommendes hænder og misbruges.*

#### **4. Princippet om anvendelsesbegrænsning**

Personlige data skal ikke afsløres, gøres tilgængelige eller på anden måde anvendes til andre formål end dem, der er specificeret, med mindre det enten er med samtykke fra den data vedrører eller sker ud fra en retslig vurdering.

*Dette fungerer som en undtagelsesbestemmelse til det ovenstående afsnit. F.eks. har vi i Danmark en række bestemmelser om, at data der er afgivet til eet formål kan anvendes i andre sammenhænge – f.eks. til forskningsbaseret statistik.*

#### **5. Princippet om sikkerhed for det indsamlede**

Personlige data skal beskyttes på fornuftig vis imod sådanne risici som tab, uautoriseret adgang, ødelæggelse, anvendelse, ændring eller afsløring.

*Data skal sikres både fysisk og logisk – herunder at de rette organisatoriske og tekniske foranstaltninger og kontroller er på plads. Alle data skal have en dataejer, der har ansvaret for datas fortrolighed.*

#### **6. Princippet om åbenhed**

Der skal være en generel åbenhed omkring udvikling i og formulering af praksisser og politikker for indsamling og anvendelse af personlige data. Der skal forefindes midler til hurtigt at fastslå eksistensen og indholdet af personlige data, formålet med deres anvendelse og identiteten og den geografiske placering af den, der administrerer data.

*For at kunne få adgang til indsamlede data er det vigtigt, at der forefindes information om, at der finder en indsamling sted, hvor den gemmes, og hvordan den bruges. Dette kan f.eks. ske ved anmeldelse til en offentlig myndighed, som vi har gjort det i Danmark, hvor denne type registre skal anmeldes til Datatilsynet.*

*At data skal være hurtigt tilgængelige betyder foruden ovenstående, at individet ikke skal bruge meget tid, ikke have speciel viden og ikke behøver at rejse for at få adgang til data.*

#### **7. Princippet om individets rettigheder**

Ethvert individ har visse rettigheder til egne data.

*Disse rettigheder betragtes som noget af det mest centrale indenfor privacy, men de kan ikke gøres absolutte i forhold til enhver tænkelig situation.*

Ethvert individ skal have ret til:

a) at kunne få data fra den, der administrerer data, eller bekræftelse på, om hvorvidt den der administrerer data er i besiddelse af data der er relateret til ham.

*Dette skal kunne gøres let for individet, være en integreret del af de daglige aktiviteter hos dataadministratoren og skal kunne foretages uden retslige handlinger. Det kan dog i visse tilfælde være relevant at data gives videre til individet via en mellemmand – f.eks. en læge der skal forklare medicinske data.*

b) at kunne modtage data, der er relateret til individet: indenfor en rimelig tid, indenfor en rimelig omkostningsramme, på en fornuftig måde og på en måde, der er forståelig for ham. *Fornuftig tid og på fornuftig måde varierer fra tilfælde til tilfælde. Som udgangspunkt regner man i dage fra begæringen er fremsat. Geografi må ikke være en forhindring for at kunne få adgang til data.*

c) at modtage begrundelse, hvis data udleveres under visse betingelse og hvis det afvises at udlevere data.

*Retten til at modtage begrundelse skal fortolkes snævert idet individet ikke kan forvente lange udredninger, hvis data ikke kan blive udleveret.*

d) at gøre indsigelse imod data, der er opbevaret om individet og hvis denne indsigelse vurderes

acceptabel at få data slettet, rettet, fuldstændiggjort eller tilføjet.

*Retten til at udfordre data er bred og dels skal individet kunne anke sagen til dataadministratoren og dels skal han have mulighed for at anke til offentlige myndigheder, professionelle organer og/eller domstolene.*

#### 8. **Princippet om ansvarlighed**

Den, der administrerer data, skal kunne holdes ansvarlig for at data er omfattet af ovenstående retningslinier.

*Dette gælder også uanset om administratoren har valgt at outsource opgaven om at behandle eller lagre data.*

Foruden selve principperne lister OECD også en række forhold, der vedrører, hvordan lovgivningen skal indrettes således, at national lovgivning ikke er til hinder for, at andre lande kan få adgang til data, som er nødvendige for dem. Her tænkes der især på politimæssigt samarbejde. Men andre former for samarbejde kan også komme på tale. Desuden er det vigtigt at data altid sikres, når de rejser på tværs af grænser og evt. opbevares i andre lande.

Yderligere fremsætter OECD ønske om, at landene retter lovgivningen til, sikrer borgernes rettigheder, opfordrer til at lave Code of Conducts, definerer konsekvenser af, hvad der skal ske, hvis guidelinen ikke overholdes og sikrer, at der ikke diskrimineres overfor individerne.

Endelig opfordrer OECD til samarbejde om at implementere guidelinen på tværs af grænserne.

Med erklæringen fra 1985 (kilde 2 ovenfor) sætter OECD fokus på, at virksomheder i stigende grad er begyndt at handle globalt via elektroniske medier. Der ses derfor et behov for at sikre, at national lovgivning og praksisser ikke er til hinder for det deraf følgende flow af data. I særdeleshed fremhæves det, at der ikke må være hindringer for:

1. flow af data som følge af international handel
2. elektroniske services på markedet
3. dataflows internt i virksomheder men på tværs af grænser.

Med erklæringen fra 1998 sættes der igen fokus på resultaterne af den øgede digitalisering, og OECD lægger derfor vægt på at privacy guidelinen implementeres i forhold til globale netværk og at medlemslandene dermed:

1. opfordrer til, at man laver privacy politikker uanset om disse implementeres i lovgivningen, fungerer gennem selv-regulering, administrativt eller teknologisk
2. opfordrer til, at man laver en online privacy politik, som tilbydes brugerne af en service
3. sikrer at der forefindes tilstrækkeligt gode organer til at håndtere, hvis guidelinen og de affødte politikker ikke efterleves med mulighed for at klage
4. fremmer brugernes uddannelse og awareness om privacy og give dem midler, der gør dem i stand til at beskytte deres privacy i globale netværk
5. opfordrer til anvendelse af privacy fremmende teknologier
6. opfordrer til at lave kontraktlige løsninger for flow af online data på tværs af grænser.

#### *Europarådet*

Samme år, som OECD fremlagde deres guidelines offentliggjorde også Europarådet sit sæt guidelines under den imponerende titel: "Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention"<sup>24</sup>. I hovedtræk berøres de samme elementer, som i OECD's

---

<sup>24</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

guidelines, men der er forskelle på enkelte punkter, hvorfor vi gennemgår det væsentligste kapitel (kapitel 2, artiklerne 4-11), "Basic principles for data protection", i konventionen. Heri hedder det:

1. Enhver relevant part skal iværksætte de foranstaltninger, som er mulige i den nationale lovgivning for at implementere konventionens bestemmelser.
2. Personhenførbare data skal indsamles på en fair måde og i overensstemmelse med lovgivningen. Data må kun lagres til anvendelse i forbindelse med specificerede og rimelige formål og ikke anvendes på en måde, der ikke er i overensstemmelse med formålet. Data skal være præcise, relevante og kun have et omfang, der står i forhold til det formål, for hvilke de gemmes. Data skal være præcise og om nødvendigt holdes opdateret. Data skal opbevares på en sådan måde, at de kun er personhenførbare i den periode, der er relevant for det formål, for hvilke de opbevares.
3. Personhenførbare data, der vedrører etnisk race, politisk holdning, religiøse overbevisning eller andre overbevisninger såvel som personhenførbare data, der vedrører helbred eller seksualliv, må ikke behandles automatisk med mindre lovgivningen sikrer disse på passende vis. Det samme skal gælde for data, der vedrører straffeattester.
4. Der skal etableres passende foranstaltninger, som sikrer personhenførbare data mod tilfældig eller uautoriseret destruktion såvel som uautoriseret adgang, ændring eller spredning.
5. Enhver person skal have retten til at fastslå eksistensen af de personhenførbare oplysninger, der er lagret - herunder formålet og hvem der er i besiddelse af dem. De pågældende data skal med rimelige intervaller og uden unødige forsinkelse eller udgifter kunne kommunikeres til den berørte person. Personen skal have ret til at få data om sig korrigeret eller slettet, hvis de ikke er i overensstemmelse med lovgivningen. Personen skal have mulighed for at anke, hvis disse bestemmelser ikke er opfyldt.
6. Ovenstående bestemmelser kan undtages, såfremt der er behov for at beskytte statens sikkerhed, offentlighedens sikkerhed, statens økonomiske interesser, forskellige kriminaliserede forhold, beskyttelse af den person, som data vedrører, andre personers frihed og statistiske og videnskabelige formål, hvor det sikres, at individernes rettigheder ikke krænkes.
7. Alle relevante parter er forpligtiget til at implementere de relevante foranstaltninger og de rette ankesmuligheder for bestemmelserne i denne konvention.
8. Ingen af konventionens bestemmelser skal ses som en begrænsning for at give den person, som data omhandler, en videre beskyttelse end angivet.

Som det ses ved at sammenligne Europarådets konvention med OECD's guidelines, er der ikke betydelige forskelle. Man kan sige, at der er sammenfald mellem Europarådets bullet 2 ovenfor og OECD's bullet 1-4, mellem Europarådets bullet 4 og OECD's bullet 5, Europarådets bullet 5 og OECD's bullet 6-7 samt Europarådets bullet 7 og OECD's bullet 8. Desuden er Europarådets bullet 1 og 8 indirekte indeholdt i OECD's guidelines. Tilbage står vi med Europarådets bullet 3 og 6. Disse adskiller sig fra OECD's guidelines ved at eksplicit gøre opmærksom på, at visse personlige informationer (f.eks. politisk, religiøs og seksuelt tilhørsforhold) er mere følsomme end andre. Desuden ved at der kan ske undtagelse fra hensynene ved en række særlige forhold (f.eks. den nationale sikkerhed). At man giver mulighed for, at visse data er mere følsomme end andre, og at der kan findes undtagelser fra de overordnede principper, synes at være en opblødning gennem konkretisering i forhold til OECD's principper.

### *EU*

Mange lande var nationalt begyndt at arbejde med privacy inden OECD og Europarådet kom med deres anbefalinger. På trods af de overordnede retningslinier, som var udstukket i de to konventioner, mente EU, at der var et behov for at harmonisere lovgivningen i EU-landene. I 1995 vedtog man derfor

Databeskyttelsesdirektivet<sup>25</sup>, som gennem lov skulle implementeres i de enkelte medlemslandes nationale lovgivning.

Direktivet har som nævnt karakter af, at skulle implementeres som national lovgivning, og er derfor betydeligt mere skarpt og præcist end de to konventioner, vi har set på ovenfor.

Man kan sige, at direktivet falder i tre afsnit. Først nogle indledende bemærkninger om fordele og ulemper ved informationsteknologi tillige med en opstilling af nogle af de fordele og ulemper, der skal afbalanceres i forhold til hinanden - herunder f.eks. retten til privatlivets fred, problemer med at udveksling af personhenførbare data kan være en handelshindring og desuden være konkurrenceforvridende, arbejdet fra Europarådet, nationale sikkerheds- og efterforskningshensyn, hensyn til sundhedsvæsenet, forskning, statistikker, pressen, kunstnere, nationale valgsystemer, personers samtykke og udpegning af nationale ansvarlige for området. Herefter følger nogle definitioner og desuden de egentlige principper, som lovgivningen skal bygge på. Endelige finder vi til sidst en række strukturelle bestemmelser om, hvordan direktivet skal implementeres, og hvordan der skal samarbejdes mellem EU-landene og mellem EU og tredjeparter.

I tråd med gennemgangen af de to konventioner vil vi også her se på de principper, der ligger til grund for direktivet. I dette tilfælde er principperne betydeligt mere præcise, idet de som nævnt skal udmøntes som national lov.

#### 1. **Principper vedrørende datakvalitet**

Data skal behandles på en fair og lovlig måde. De må kun indsamles til et specifikt præciseret og lovligt formål, og må kun behandles i overensstemmelse med dette formål. Data må dog godt senere anvendes til historiske, statistiske eller videnskabelige formål, såfremt de beskyttes passende. Data skal være passende, relevante og ikke i omfang være mere omfattende, end det er relevant for det formål, hvortil de indsamles. Data skal være præcise, og hvor det skønnes nødvendigt være opdateret. Det skal sikres, at data som er upræcise eller ukomplette slettes eller korrigeres under hensyntagen til formålet. Data skal opbevares på en sådan måde, at de kun er personhenførbare i den periode, hvor det er relevant for formålet.

#### 2. **Principper for hvornår der må foretages behandling af personhenførbare data**

Behandling af personhenførbare data må kun finde sted, hvis et af nedenstående forhold er opfyldt:

- den data vedrører har givet sit tilsagn
- det er nødvendigt for behandling af en kontrakt, hvori den data vedrører er part
- det er nødvendigt for udøvelse af lovgivningen
- det er afgørende nødvendigt af hensyn til den data vedrører
- det er nødvendigt for udførelse af en opgave, som er i offentlighedens interesse, eller er en del af den offentlige administration.

#### 3. **Speciel kategorisering af behandling af data**

Der må ikke finde behandling af data sted, som angiver racemæssig eller etnisk oprindelse, politiske holdninger, religiøs eller filosofisk overbevisning, fagforeningsmedlemskab, helbredsmæssig tilstand eller seksuelle præferencer. Til denne bestemmelse findes en række undtagelser som vedrører a) retten til at hæve ovenstående gennem samtykke, hvis dette er lovligt, b) arbejdsmarkedsretlige regler, c) beskyttelse af den som data vedrører eller andre individer, i de særlige situationer, hvor den pågældende er afskåret fra at give samtykke, d) foreningers virke indenfor de ovennævnte områder, e) allerede offentlige data om den data

---

<sup>25</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:HTML>

vedrører eller data som er relevant for udøvelse af lovgivning, f) sygdoms- og sundheds behandling, g) speciel national lovgivning, h) oplysninger om kriminelle forhold og i) oplysninger i form af anvendelse af personnumre.

Undtagelser, som vedrører særlig national eller oplysninger om kriminelle forhold, skal meddeles EU-kommissionen af den pågældende nationalstat.

I national lovgivning kan der findes særlige bestemmelser for anvendelse af personhenførbare data i forbindelse med journalistisk, kunstnerisk eller litterært virke.

#### 4. **Information som skal videregives til den som data vedrører**

Når der indsamles data fra en person, skal denne som minimum informeres om, hvem der indsamler data, formålet hvormed data indsamles, hvem der modtager data, om data afgives frivilligt eller obligatorisk og personens ret til at få adgang til de pågældende data og eventuelt rette dem.

Hvis data ikke er indsamlet direkte fra den person, som data omhandler, skal det sikres, at den pågældende person får adgang til de samme oplysninger (jf. ovenfor), som hvis data var indsamlet direkte hos ham. Undtagelse herfra er dog data, der anvendes til statistiske, historiske eller forskningsmæssige formål.

#### 5. **Ret til adgang til egne personlige data**

Enhver person skal indenfor rimelig tid og uden nævneværdige omkostninger, fra den der kontrollerer data, kunne få oplyst, om der findes personlige data om ham eller ej. I bekræftende fald skal det også oplyses, hvad formålet er, hvilke kategorier data tilhører, og hvem der modtager data. Desuden skal den data vedrører kunne få adgang til data, få at vide hvorfra de stammer (kilden) og få indsigt i den automatik, data eventuelt bliver behandlet med. Desuden skal der i visse tilfælde være adgang til at få korrigeret eller slettet data eller blokeret for datas overførsel til tredjepart. Såfremt data er udleveret til tredjepart, skal eventuelle rettelser også slå igennem her, medmindre det må anses for at være for omfattende.

#### 6. **Undtagelser og begrænsninger**

De ovenfor nævnte principper kan afviges med national lovgivning, hvis der er tale om forhold, som vedrører national sikkerhed, forsvar, offentlighedens sikkerhed, forebyggelse, undersøgelse, opklaring og retsforfølgelse af kriminelle forhold, er af betydelig økonomisk betydning for landets økonomi, udføres rutinemæssigt i forbindelse med offentlige opgaver, beskyttelse af den person som data vedrører eller andres frihedsrettigheder og endelig i visse sammenhænge til statistiske eller forskningsmæssige formål.

#### 7. **Klagemuligheder for den som data vedrører**

Den, som data vedrører, skal altid have klageret i de tilfælde, hvor data behandles som et led i udførelsen af offentlige opgaver, hvis oplysninger gives videre til tredjeparter og hvis databehandlingen sker med henblik på markedsføring.

Ingen person må blive betydeligt skadet af informationer, der er baseret alene på en automatiseret behandling af data.

#### 8. **Fortrolighed og sikkerhed i forbindelse med behandling af data**

Kun den, der har ansvaret for data eller den som handler på baggrund af lovgivning, skal have ret til at behandle personlige data.

Det skal sikres, at data er behørigt beskyttet mod uheld, ulovlig ødelæggelse, tilfældige tab, ændring og uautoriseret afsløring eller adgang. Dette gælder også, hvor databehandlingen er outsourcet.

#### 9. **Anmeldelse af databehandling**

Der skal ske anmeldelse og indhentes tilladelse til behandling af personlige data fra en overordnet eller central myndighed. For at gøre dette operationelt anføres en række bestemmelser, som skal lette eller undtage denne anmeldelse af databehandling.

Når anmeldelsen skal gives, skal den mindst indeholde: navn på den som er ansvarlig for behandlingen af data, formålet hvormed databehandlingen finder sted, beskrivelse af dem, som

der indhentes data om tillige med en beskrivelse af hvilke data som indhentes, redegørelse for hvem der modtager data – herunder tredjeparter i ind- og udland og beskrivelse af sikkerheden omkring data.

Myndighederne skal på denne baggrund vurdere, om der er risici for krænkelse af de personer som data vedrører.

Det skal være synligt, hvordan data behandles, og dette skal kontrolleres af myndighederne.

Foruden disse principper, som skal implementeres i national lovgivning, omtaler databeskyttelsesdirektivet også en række andre forhold. Det vedrører blandt andet, at der skal etableres en central uafhængig myndighed, som administrerer loven, overførsel af persondata på tværs af nationale grænser, samarbejde på tværs af grænser (blandt andet nedsættelse af artikel 29 gruppen<sup>26</sup>), mulighederne for at brancher kan etablere specielle Code of Conducts for at regulere deres egen branche.

En meget interessant paragraf i direktivet viser, at såfremt den teknologiske udvikling på et givent område er nået tilstrækkeligt langt, og de økonomiske omkostninger ikke er prohibitive, bør man gå efter en privacyenabling af de tekniske løsninger: ”Beskyttelsen af de registreredes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger forudsætter, at der træffes de fornødne tekniske og organisatoriske foranstaltninger både under selve udformningen og under iværksættelsen af en behandling, navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet behandling; det påhviler medlemsstaterne at sørge for, at de registeransvarlige overholder disse foranstaltninger; disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, der skal beskyttes”<sup>27</sup>. Pointen om at anvende privacyfremmende teknologier slås også fast andre steder af EU: ”Kun de data, der er nødvendige for at opfylde et givet formål, må indsamles. Til dette formål bør brugen af privatlivsbeskyttende teknologier fremmes ... Privatlivsbeskyttende teknologier bør styrkes i forbindelse med e-forvaltning, bl.a. gennem de relevante EU-programmer ... Adgang til oplysninger om borgerne skal være i fuld overensstemmelse med EU's og medlemsstaternes lovgivning om databeskyttelse, og der bør vælges den teknologi, der i størst mulig grad lader borgerne bevare kontrollen over persondata vedrørende dem selv”<sup>28</sup>.

EU har også på andre fronter beskæftiget sig med forhold, der vedrører privacy. I Europa-Kommissionens meddelelse om ”i2010 – Et europæisk informationsfund som middel til vækst og beskæftigelse” foreslås en ny strategisk ramme, der udstikker nye, politiske retningslinier for udvikling af det europæiske informationsfund. Som led i dette er en række direktiver knyttet til digital kommunikation aktuelt under revision<sup>29</sup>. Privacy indgår bl.a. i direktivet Privacy and Electronic Communications 2002/58/EC<sup>30</sup>.

### *Danmark*

Persondataloven<sup>31</sup> er den danske lov, som implementerer EU's databeskyttelsesdirektiv. Den trådte i kraft pr. 1 juli 2000 og afløste ved denne lejlighed registerloven. Loven indeholder seks hovedafsnit:

---

<sup>26</sup> Artikel 29 gruppen består af en repræsentant fra hver nationalstat i EU. Gruppen koordinerer persondatabeskyttelse i EU, udveksler best practices, fortæller om verserende sager og afholder høringer og kommenterer nye teknologier.

<sup>27</sup> <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:HTML>, artikel 46.

<sup>28</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:DA:HTML>

<sup>29</sup> Se opsummering fra Ministeriet for Videnskab, teknologi og Udvikling: [www.videnskabsministeriet.dk/cgi-bin/doc-show.cgi?doc\\_id=253770&doc\\_t](http://www.videnskabsministeriet.dk/cgi-bin/doc-show.cgi?doc_id=253770&doc_t).

<sup>30</sup> <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:DA:HTML>.

<sup>31</sup> <http://www.datatilsynet.dk/lovgivning/personoplysninger/indhold.asp>

- Indledende bestemmelser
- Behandlingsregler
- Registreredes rettigheder
- Sikkerhed
- Anmeldelse
- Tilsyn og afsluttende bestemmelser

Datatilsynet har lavet en udmærket pjece, som beskriver hovedindholdet i loven<sup>32</sup>.

Vi vil i det følgende gennemgå loven i hovedtræk for at identificere de principper, der ligger bag loven, og i helt overordnede træk at se på, hvordan de væsentligste af disse er implementeret i praksis.

### 1. **Indledende bestemmelser**

De indledende bestemmelser indeholder lovens område, definitioner af de begreber, der anvendes i loven, og endelig en beskrivelse af, hvilket geografisk område loven dækker. Vi ser her kun på lovens omfang.

Udgangspunktet er at "Loven gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register"<sup>33</sup>. Loven gælder også for systematisk behandling af oplysninger om private og i visse tilfælde virksomheder. Der er en række undtagelser til, hvad loven ikke omfatter. Dette er fortrinsvis: a) anden lovgivning, som giver bedre retsstilling, b) eventuel strid med Menneskerettighedskonventionens artikel 10 om ytringsfrihed, c) aktiviteter af rent privat karakter, d) domstole, politi og anklagemyndighed i forbindelse med strafferetlige sager, e) folketinget, f) massemedier og journalistisk arbejde og g) PET og FET.

### 2. **Behandlingsregler**

Behandlingen af data skal finde sted i overensstemmelse med god databehandlingsskik. Dette omfatter a) på forhånd angivne og saglige formål, b) forenelighed med oprindeligt formål for indsamling, c) kun de oplysninger der er nødvendige for opfyldelse af formålet, d) opdatering af oplysninger, så de er tidssvarende, e) data skal slettes eller anonymiseres når det ikke længere er nødvendigt for formålet at bevare data.

Behandling af data må kun finde sted hvis: a) der er givet samtykke, b) det er nødvendigt for en aftale, c) det sker for at overholde en retslig forpligtelse, d) der er vitale interesser for den data vedrører, e) det er i samfundets interesse, f) det sker som led i offentlig myndighedsudøvelse, g) der er berettiget interesse for den, der er i besiddelse af data, og hvor hensynet til den, som data vedrører, ikke overstiges.

I de følgende paragraffer ligger der en ret implicit klassifikation af data, som understøttes af bemærkningerne til lovforslaget, efter grad af følsomhed. Der tales i loven kun om en sondring imellem følsomme og andre personhenførbare data. I praksis må det antages at loven skal fortolkes som omhandlende flere klasser af data ligesom konteksten, hvori data indgår er af væsentlig betydning. I dette notat ser vi kun på lovens definition af følsomme data, vel vidende at man formodentlig i praksis vil kunne tale om en mellemkategori af fortrolige data:

- **Følsomme data**

Der må ikke behandles oplysninger (§ 7) om race, etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold eller helbreds- og seksuelle forhold med mindre der foreligger samtykke, beskyttelse af vitale interesser hvor samtykke ikke er muligt, den data vedrører selv har offentliggjort oplysningerne

<sup>32</sup> <http://www.datatilsynet.dk/publikationer/pjece/persondataloven.htm>

<sup>33</sup> Lov om behandling af personoplysninger, §1, stk. 1.

eller hvis det er nødvendigt i forhold til retskrav. Der er visse undtagelser herfor, som vi ikke vil berøre.

Der må heller ikke behandles oplysninger (§ 8) om strafbare forhold, væsentlige sociale problemer, andre rent private forhold (f.eks. selvmordsforsøg, registreret partner, bortvisning fra job, personlighedstests) med mindre samtykke eller en af de andre ting foreligger. Igen er der enkelte undtagelser.

Der er desuden en række andre regler for behandlingen af disse typer data. Bl.a. at data må behandles i forbindelse med retsinformation (§ 9) samt ved statistiske og videnskabelige formål (§ 10).

Af øvrige behandlingsregler kan det fremhæves, at der er særlige regler for virksomheder, der sælger adresselister eller kuverterer (§ 12), arbejdsgivers registrering af telefonopkald (§ 13), forhold til arkivlovgivningen (§ 14), videregivelse af oplysninger om gæld til det offentlige (§§ 16-18), kreditoplysningsbureauer (§§ 19-26) samt overførsel af oplysninger til tredjelande (§ 27).

### **3. Registreredes rettigheder**

Ved indsamling af data skal der gives oplysninger om: identiteten af den dataansvarlige og den der indsamler data, formålet med behandlingen af data og supplerende oplysninger for at den, som data vedrører, kan varetage sine egne interesser. De samme oplysninger skal gives til den data vedrører, hvis data indsamles hos en tredjepart eller videregives til en tredjepart. Der er dog visse undtagelser fra disse regler – f.eks. hvis den data vedrører allerede er bekendt med indsamlingen, hvis underretning er uforholdsmæssig vanskelig, bør vige for private interesser, statens sikkerhed, forsvaret, den offentlige sikkerhed, relation til straffesager, væsentlige økonomiske statslige interesser eller offentlig myndighedsudøvelse.

Den person som data vedrører har indsigtret, og den dataansvarlige skal altid kunne give den pågældende person meddelelse om, hvorvidt der behandles oplysninger om vedkommende – herunder: hvilke oplysninger der behandles, med hvilket formål, kategorierne af modtagere af oplysningerne og tilgængelig information om hvorfra oplysningerne stammer. Svar skal ske indenfor fire uger. Undtagelserne fra dette svarer til dem, der gælder ved indsamling af data tillige med et par ekstra undtagelser.

Der kan højst kræves indsigt i oplysninger hver 6. måned, og der kan kræves rimelig betaling for indsigten.

Den, som data vedrører, kan altid overfor den dataansvarlige gøre indsigelse mod, at vedkommende gøres til genstand for behandling. Den dataansvarlige skal berigtige, blokere eller slette urigtige eller vildledende oplysninger.

Den, som oplysningerne vedrører, kan tilbagekalde et samtykke. Hvis der kan klages, kan der ikke træffes afgørelser, der har retsvirkning alene på baggrund af elektronisk behandling, med mindre særlige forhold er opfyldt (der skal altså ske manuel behandling af data). Den, som data vedrører, kan altid klage til en tilsynsmyndighed.

### **4. Sikkerhed**

Databehandleren handler altid efter instruks fra den dataansvarlige (§ 41). Dette må dog ikke begrænse den journalistiske frihed eller skabelsen af et kunstnerisk eller litterært produkt.

Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere<sup>34</sup>.

Oplysninger, som er af særlig interesse for fremmede magter, skal kunne bortskaffes eller tilintetgøres i tilfælde af krig eller lignende forhold.

---

<sup>34</sup> Lov om behandling af personoplysninger, § 41, stk. 2.

Den dataansvarlige skal sikre, at databehandleren kan efterleve ovenstående sikkerhedsbestemmelser, og aftalen de to imellem skal foreligge skriftligt.

#### 5. **Anmeldelse**

Inden den offentlige forvaltning begynder at behandle oplysninger, skal dette anmeldes til Datatilsynet. Anmeldelsen skal indeholde a) navn og adresse på den dataansvarlige og eventuel databehandler, b) behandlingens betegnelse og formål, c) en generel beskrivelse af behandlingen, d) en beskrivelse af kategorierne af registrerede og de typer af oplysninger der vedrører dem, e) modtagere eller kategorier af modtagere, som oplysningerne kan overføres til, f) påtænkte overførsler af oplysninger til tredjelande, g) beskrivelse af foranstaltninger, der iværksættes af hensyn til behandlingssikkerheden, h) tidspunktet for påbegyndelsen af behandlingen, i) tidspunktet for sletning af oplysningerne. En række undtagelsesbestemmelser nævnes.

Foruden anmeldelsen skal der indhentes udtalelse forinden anmeldelsen, når der er tale om følsomme oplysninger, retsinformation, forskning og statistik eller samkøring i kontroløjemed. Der er tale om stort set de samme regler, når en privat dataansvarlig indsamler og behandler personoplysninger. Dog er rækken af undtagelser i dette tilfælde langt større, idet der bl.a. tages hensyn til forhold på arbejdsmarkedet, forretningsforbindelser og foreninger.

Der er desuden en lang række specielle krav for indhentning af tilladelse for private og særlige offentlige databehandlere.

Datatilsynet skal føre en liste over de behandlinger, der er anmeldt, og listen skal være tilgængelig for offentligheden (§ 54).

#### 6. **Tilsyn og afsluttende bestemmelser**

I lovens sidste afsnit beskrives Datatilsynets organisering (herunder præciseres det, at Datatilsynet er uafhængigt), Datatilsynets beføjelser (herunder at tilsynet kan kræve enhver oplysning af betydning for dets virksomhed og uden retskendelse har adgang til alle lokaliteter, hvor der behandles personoplysninger), gebyrer for anmeldelse m.v., Datatilsynets eksterne relationer (f.eks. med andre medlemsstaters tilsyn samt domstolsstyrelsen) samt erstatnings- og strafansvar for den dataansvarlige.

I dette afsnit beskrives det også, hvordan brancheorganisationer sammen med Datatilsynet kan udarbejde kodekser, som gør det lettere for erhvervslivet at efterleve persondataloven:

”Brancheforeninger eller andre organer, som repræsenterer andre kategorier af private dataansvarlige, kan i samarbejde med Datatilsynet udarbejde adfærdskodekser, der skal bidrage til en korrekt anvendelse af reglerne i denne lov”<sup>35</sup>.

Det skal bemærkes, at der ved siden af persondataloven findes anden lovgivning, som vedrører privacy – enten ved at give en bedre eller en ringere retsstilling til borgerne. Vi kan i dette notat ikke berøre disse andre typer lovgivning.

Det skal også bemærkes, at informationsteknologien giver mulighed for en omfattende sammenkædning af fysiske personer, juridiske personer (f.eks. virksomheder) og genstande (f.eks. produkter med serienummer/registreringsnummer), således at en meget stor mængde information kan relateres til et enkelt individ, selvom informationen efter lovens bogstav ikke er personhenførbart. Dette understreger behovet for privacy-principper, der rækker videre end den gældende lovgivning.

### **Sammenfatning af principper**

Vi kan nu på baggrund af ovenstående lave en endegyldig identifikation af de principper, som ifølge de gennemgåede kilder påvirker privacy:

---

<sup>35</sup> Lov om behandling af personoplysninger, § 74

## PRINCIPPER

- Borgerne bør som grundprincip have **kontrol** med egne data og identiteter.
- **Indsamling** af data skal foregå begrænset på en fair måde, være i overensstemmelse med lovgivningen og med både viden og accept/samtykke fra den person data vedrører. Indsamling kan kun finde sted, når den data vedrører har givet tilsagn, er omfattet af en kontrakt, som betinger indsamling, når loven kræver det, når det sker af hensyn til den data vedrører og ved udførelse af offentlig myndighedsudøvelse.
- Hvis indsamlede data **videregives** til tredjepart, skal den data vedrører oplyses herom på rimelig måde.
- Indsamlede data skal i snæver fortolkning anvendes begrænset og i overensstemmelse med det **formål**, til hvilke de er indsamlet og data må ikke anvendes/afsløres til noget andet formål. Når formålet evt. måtte **ændres** skal data destrueres eller anonymiseres.
- Indsamlede data skal til enhver tid have en god **kvalitet** hvilket indebærer, at de er præcise, komplette og opdaterede.
- Den, som data vedrører, har altid **ret til egne data** og kan altid kræve **indsigt** i om data er registret af en bestemt enhed og i givet fald, hvilke data der er registret, hvad de anvendes til, med hvilket formål og hvor de lagres. Disse oplysninger skal afgives indenfor en **rimelig tid**, til en **rimelig pris** og på en **forståelig måde**. Den, som behandler data, skal dermed udvise **åbenhed** overfor den, som data vedrører. Såfremt data udleveres under givne **betingelser**, skal disse begrundes. De, som data vedrører, kan også kræve **retslig prøvelse** af sammenhæng mellem data og formål, datas kvalitet, manglende efterlevelse af offentliggjorte privacypolitikker og eventuelle begrundelse for betingelser. Retten til at kræve oplysninger udleveret er dog **begrænset tidsmæssigt**, således at det maksimalt kan ske hver sjette måned.
- Den som lagrer og behandler data er altid **ansvarlig** for data og disses **sikkerhed** - herunder tilfældig eller uautoriseret destruktion, adgang, ændring eller spredning.
- Der skal i det omfang det er muligt - under hensynet til rettighederne hos den som data vedrører - **ikke være begrænsninger for flow af data** ved international handel, anvendelse af elektroniske services og dataflow internt i virksomheder på tværs af grænser. Disse forhold bør i videst muligt omfang løses gennem **kontrakter**.
- Privacyforanstaltninger skal implementeres under hensyn til det aktuelle **tekniske niveau** og de omkostninger, som er forbundet med deres iværksættelse.
- Den, som indsamler og behandler data, bør i videst muligt omfang tilvejebringe offentlige og gennemskuelige **privacypolitikker** og tilsikre, at den, som data vedrører, er bekendt med og har accepteret disse.
- Når behandling af personhenførbare oplysninger finder sted, skal der ske **anmeldelse** til Datatilsynet.

## UNDTAGELSER

- Undtagelser fra ovenstående gælder i en række konkrete sammenhænge i forbindelse med bl.a. statens og offentlighedens sikkerhed, statens økonomiske interesser, kriminelle forhold, beskyttelse af den data vedrører, andre personers frihed, samt historisk, journalistisk, videnskabelig samt statistisk bearbejdelse.
- Undtagelser gælder også i forbindelse med behandling af særligt følsomme data (etnisk race, politisk holdning, religiøs, filosofisk eller anden overbevisning, helbred, seksuelle eller straffemæssige forhold), ved samtykke til behandling, arbejdsmarkedsforhold, foreninger, allerede offentliggjorte data, behandling af sygdomme og særlig national lovgivning.
- Videre beskyttelse end skitseret ovenfor er altid muligt.

Det skal afslutningsvis bemærkes, at loven kun er et minimum for den privacy, der skal gives. Bedre privacy kan gives! Næsten alle principperne har en indbygget gradbøjning af begrænsninger og foranstaltninger i forhold til de aktuelle risici. Tilsvarende kan definitionerne af begreberne fortolkes forskelligt afhængigt af kontekst. For at være sikker på, at være dækket ind i forhold til privacy er det derfor nødvendigt med en klassifikation - ikke blot af data og risici - men også af processer, systemer, scenarier og transaktioner.